Sadržaj: Pojam kriptologije. Svrha kriptologije. Istorijat, dometi i budućnost kriptologije.Teorijske osnove. Prosti šifarski sistemi, moderne protočne šifre i konačna polja. Pojam sigurnosti kriptosistema, napadi na blokovske šifre. Simetrični kriptosistemi, AES, DES, triple-DES. Kriptosistemi sa javnim ključem: RSA. Heš funkcije, MD5, kodovi za autentifikaciju, potpisi za autentifikaciju. Kriptoanaliza. Linearna i diferencijalna kriptoanaliza. Ispitivanje prostosti broja, faktorizacija brojeva. Načini odabira tajnog ključa. Permutacioni polinomi, kriptologije upotrebom eliptičkih krivih. Booleove funkcije.